

# THE MINIMUM DISTANCE OF PARAMETERIZED CODES ON PROJECTIVE TORI

ELISEO SARMIENTO, MARIA VAZ PINTO, AND RAFAEL H. VILLARREAL

**ABSTRACT.** Let  $X$  be a subset of a projective space, over a finite field  $K$ , which is parameterized by the monomials arising from the edges of a clutter. Let  $I(X)$  be the vanishing ideal of  $X$ . It is shown that  $I(X)$  is a complete intersection if and only if  $X$  is a projective torus. In this case we determine the minimum distance of any parameterized linear code arising from  $X$ .

## 1. INTRODUCTION

Let  $K = \mathbb{F}_q$  be a finite field with  $q$  elements and let  $y^{v_1}, \dots, y^{v_s}$  be a finite set of monomials. As usual if  $v_i = (v_{i1}, \dots, v_{in}) \in \mathbb{N}^n$ , then we set

$$y^{v_i} = y_1^{v_{i1}} \cdots y_n^{v_{in}}, \quad i = 1, \dots, s,$$

where  $y_1, \dots, y_n$  are the indeterminates of a ring of polynomials with coefficients in  $K$ . Consider the following set parameterized by these monomials

$$X := \{[(x_1^{v_{11}} \cdots x_n^{v_{1n}}, \dots, x_1^{v_{s1}} \cdots x_n^{v_{sn}})] \in \mathbb{P}^{s-1} \mid x_i \in K^* \text{ for all } i\},$$

where  $K^* = K \setminus \{0\}$  and  $\mathbb{P}^{s-1}$  is a projective space over the field  $K$ . Following [20] we call  $X$  an *algebraic toric set* parameterized by  $y^{v_1}, \dots, y^{v_s}$ . The set  $X$  is a multiplicative group under componentwise multiplication.

Let  $S = K[t_1, \dots, t_s] = \bigoplus_{d=0}^{\infty} S_d$  be a polynomial ring over the field  $K$  with the standard grading, let  $[P_1], \dots, [P_m]$  be the points of  $X$ , and let  $f_0(t_1, \dots, t_s) = t_1^d$ . The *evaluation map*

$$(1.1) \quad \text{ev}_d: S_d = K[t_1, \dots, t_s]_d \rightarrow K^{|X|}, \quad f \mapsto \left( \frac{f(P_1)}{f_0(P_1)}, \dots, \frac{f(P_m)}{f_0(P_m)} \right)$$

defines a linear map of  $K$ -vector spaces. This map is well defined, i.e., it is independent of the choice of representatives  $P_1, \dots, P_m$ . The image of  $\text{ev}_d$ , denoted by  $C_X(d)$ , defines a *linear code*. Following [17] we call  $C_X(d)$  a *parameterized code* of order  $d$ . As usual by a *linear code* we mean a linear subspace of  $K^{|X|}$ .

The definition of  $C_X(d)$  can be extended to any finite subset  $X \subset \mathbb{P}^{s-1}$  of a projective space over a field  $K$ . Indeed if we choose a degree  $d \geq 1$ , for each  $i$  there is  $f_i \in S_d$  such that  $f_i(P_i) \neq 0$  and we can define  $C_X(d)$  as the image of the evaluation map given by

$$\text{ev}_d: S_d = K[t_1, \dots, t_s]_d \rightarrow K^{|X|}, \quad f \mapsto \left( \frac{f(P_1)}{f_1(P_1)}, \dots, \frac{f(P_m)}{f_m(P_m)} \right).$$

In this generality—the resulting linear code— $C_X(d)$  is called an *evaluation code* associated to  $X$  [9]. It is also called a *projective Reed-Muller code* over the set  $X$  [5, 12]. Some families of

2000 *Mathematics Subject Classification.* Primary 13P25; Secondary 14G50, 14G15, 11T71, 94B27, 94B05.

The first author was partially supported by CONACyT. The second author is a member of the Center for Mathematical Analysis, Geometry and Dynamical Systems. The third author was partially supported by CONACyT grant 49251-F and SNI.

evaluation codes—including several variations of Reed-Muller codes—have been studied extensively using commutative algebra methods (e.g., Hilbert functions, resolutions, Gröbner bases), see [4, 5, 9, 10, 12, 17, 18, 19, 23]. In this paper we use these methods to study parameterized codes over finite fields. There are some other papers that have studied evaluation codes from the commutative algebra perspective [3, 14, 26].

The *dimension* and the *length* of  $C_X(d)$  are given by  $\dim_K C_X(d)$  and  $|X|$  respectively. The dimension and the length are two of the *basic parameters* of a linear code. A third basic parameter is the *minimum distance* which is given by

$$\delta_d = \min\{\|v\| : 0 \neq v \in C_X(d)\},$$

where  $\|v\|$  is the number of non-zero entries of  $v$ . The basic parameters of  $C_X(d)$  are related by the *Singleton bound* for the minimum distance:

$$\delta_d \leq |X| - \dim_K C_X(d) + 1.$$

The parameters of evaluation codes over finite fields have been computed in a number of cases. If  $X = \mathbb{P}^{s-1}$ , the parameters of  $C_X(d)$  are described in [23, Theorem 1]. If  $X$  is the image of the affine space  $\mathbb{A}^{s-1}$  under the map  $\mathbb{A}^{s-1} \rightarrow \mathbb{P}^{s-1}$ ,  $x \mapsto [(1, x)]$ , the parameters of  $C_X(d)$  are described in [4, Theorem 2.6.2]. Lower bounds for the minimum distance of evaluation codes have been shown when  $X$  is any complete intersection reduced set of points in a projective space [3, 9, 14], and when  $X$  is a reduced Gorenstein set of points [26]. Upper bounds for the minimum distance of certain parameterized codes are given in [17, 21]. In this paper we examine the case when  $X$  is an algebraic toric set parameterized by  $y_1, \dots, y_s$ .

The contents of this paper are as follows. In Section 2 we introduce the preliminaries and explain the well known connection—via Hilbert functions—between the invariants of the vanishing ideal of  $X$  and the parameters of  $C_X(d)$ , all the results of this section are well known. In Section 3 we recall a classical and well known upper bound for the number of roots of a non-zero polynomial in  $S$  (see Lemmas 3.1 and 3.2). Then, we show upper bounds for the number of roots, over an affine torus, for a certain family of polynomials in  $S$  (see Theorem 3.4). The main theorem of Section 3 is a formula for the minimum distance of  $C_X(d)$ , where

$$X = \{[(x_1, \dots, x_s)] \in \mathbb{P}^{s-1} \mid x_i \in K^* \text{ for all } i\}$$

is a *projective torus* in  $\mathbb{P}^{s-1}$  (see Theorem 3.5). Evaluation codes associated to a projective torus are called *generalized projective Reed-Solomon* codes [11]. If  $X$  is a projective torus in  $\mathbb{P}^1$  or  $\mathbb{P}^2$ , we recover some formulas of [11, 17] for the minimum distance of  $C_X(d)$  (see Proposition 3.6).

Let  $X$  be an algebraic toric set parameterized by  $y^{v_1}, \dots, y^{v_s}$ . The *vanishing ideal* of  $X$ , denoted by  $I(X)$ , is the ideal of  $S$  generated by the homogeneous polynomials of  $S$  that vanish on  $X$ . The ideal  $I(X)$  is called a *complete intersection* if it can be generated by  $s-1$  homogeneous polynomials of  $S$ . In what follows we assume that  $v_1, \dots, v_s$  are the characteristic vectors of the edges of a clutter (a special sort of hypergraph, see Definition 4.1). In Section 4 we are able to classify when  $I(X)$  is a complete intersection (see Theorem 4.4 and Corollary 4.5). The main algebraic fact about  $I(X)$  that we need for this classification is a remarkable result of [17] showing that  $I(X)$  is a binomial ideal.

The complete intersection property of  $I(X)$  has also been studied in [21], but from a linear algebra perspective. Let  $\phi: \mathbb{Z}^n/L \rightarrow \mathbb{Z}^n/L$  be the multiplication map  $\phi(\bar{a}) = (q-1)\bar{a}$ , where  $L$  is the subgroup generated by  $\{v_i - v_1\}_{i=2}^s$ . In [21] it is shown that if the clutter is uniform, i.e., all its edges have the same cardinality, and  $q \geq 3$ , then  $I(X)$  is a complete intersection if and only if  $v_1, \dots, v_s$  are linearly independent and the map  $\phi$  is injective.

We show an optimal upper bound for the regularity of  $I(X)$  in terms of the regularity of a complete intersection (see Proposition 4.6). This shows that the complete intersection  $I(X)$  from clutters have the largest possible regularity.

The ideal  $I(X)$  is studied in [21] from the viewpoint of computational commutative algebra. The degree-complexity and the reduced Gröbner basis of  $I(X)$ , with respect to the reverse lexicographical order, is examined in [21, Theorem 4.1].

For all unexplained terminology and additional information we refer to [7] (for the theory of binomial ideals), [1, 24] (for the theory of polynomial ideals and Hilbert functions), [16, 25, 27] (for the theory of error-correcting codes and algebraic geometric codes), and [17] (for the theory of parameterized codes).

## 2. PRELIMINARIES: HILBERT FUNCTIONS AND THE BASIC PARAMETERS OF CODES

We continue to use the notation and definitions used in the introduction. In this section we introduce the basic algebraic invariants of  $S/I(X)$ , via Hilbert functions, and we recall their well known connection with the basic parameters of parameterized linear codes. Then, we present some of the results that will be needed later.

Recall that the *projective space* of dimension  $s - 1$  over  $K$ , denoted by  $\mathbb{P}^{s-1}$ , is the quotient space

$$(K^s \setminus \{0\}) / \sim$$

where two points  $\alpha, \beta$  in  $K^s \setminus \{0\}$  are equivalent if  $\alpha = \lambda\beta$  for some  $\lambda \in K^*$ . We denote the equivalence class of  $\alpha$  by  $[\alpha]$ . Let  $X \subset \mathbb{P}^{s-1}$  be an algebraic toric set parameterized by  $y^{v_1}, \dots, y^{v_s}$  and let  $C_X(d)$  be a parameterized code of order  $d$ . The kernel of the evaluation map  $\text{ev}_d$ , defined in Eq. (1.1), is precisely  $I(X)_d$  the degree  $d$  piece of  $I(X)$ . Therefore there is an isomorphism of  $K$ -vector spaces

$$S_d/I(X)_d \simeq C_X(d).$$

It is well known that two of the basic parameters of  $C_X(d)$  can be expressed using Hilbert functions of standard graded algebras [5, 12, 17, 23], as we now explain. Recall that the *Hilbert function* of  $S/I(X)$  is given by

$$H_X(d) := \dim_K (S/I(X))_d = \dim_K S_d/I(X)_d = \dim_K C_X(d).$$

The unique polynomial  $h_X(t) = \sum_{i=0}^{k-1} c_i t^i \in \mathbb{Z}[t]$  of degree  $k - 1 = \dim(S/I(X)) - 1$  such that  $h_X(d) = H_X(d)$  for  $d \gg 0$  is called the *Hilbert polynomial* of  $S/I(X)$ . The integer  $c_{k-1}(k-1)!$ , denoted by  $\deg(S/I(X))$ , is called the *degree* or *multiplicity* of  $S/I(X)$ . In our situation  $h_X(t)$  is a non-zero constant because  $S/I(X)$  has dimension 1. Furthermore  $h_X(d) = |X|$  for  $d \geq |X| - 1$ , see [15, Lecture 13]. This means that  $|X|$  is the *degree* of  $S/I(X)$ . Thus,  $H_X(d)$  and  $\deg(S/I(X))$  are the dimension and the length of  $C_X(d)$  respectively.

There are algebraic methods, based on elimination theory and Gröbner bases, to compute the dimension and the length of  $C_X(d)$  [17]. This is one of the reasons that make some of the basic parameters of parameterized codes more tractable. However, in general, the problem of computing the minimum distance of a linear code is difficult because it is NP-hard [28].

The *index of regularity* of  $S/I(X)$ , denoted by  $\text{reg}(S/I(X))$ , is the least integer  $p \geq 0$  such that  $h_X(d) = H_X(d)$  for  $d \geq p$ . The degree and the regularity index can be read off the Hilbert series as we now explain. The Hilbert series of  $S/I(X)$  can be written as

$$F_X(t) := \sum_{i=0}^{\infty} H_X(i) t^i = \sum_{i=0}^{\infty} \dim_K (S/I(X))_i t^i = \frac{h_0 + h_1 t + \dots + h_r t^r}{1 - t},$$

where  $h_0, \dots, h_r$  are positive integers. Indeed  $h_i = \dim_K(S/(I(X), t_s))_i$  for  $0 \leq i \leq r$  and  $\dim_K(S/(I(X), t_s))_i = 0$  for  $i > r$ . This follows from the fact that  $I(X)$  is a Cohen-Macaulay lattice ideal of height  $s - 1$  [17], and by observing that  $\{t_s\}$  is a regular system of parameters for  $S/I(X)$  (see [24]). The number  $r$  is the regularity index of  $S/I(X)$  and  $h_0 + \dots + h_r$  is the degree of  $S/I(X)$  (see [29, Corollary 4.1.12]). In our situation,  $\text{reg}(S/I(X))$  is the Castelnuovo-Mumford regularity of  $S/I(X)$  [6]. We will refer to  $\text{reg}(S/I(X))$  as the *regularity* of  $S/I(X)$ .

For convenience we recall the following result on complete intersections.

**Proposition 2.1.** [11, Theorem 1, Lemma 1] *If  $\mathbb{T} = \{(x_1, \dots, x_s) \in \mathbb{P}^{s-1} \mid x_i \in K^* \text{ for all } i\}$  is a projective torus in  $\mathbb{P}^{s-1}$ , then*

- (a)  $I(\mathbb{T}) = (\{t_i^{q-1} - t_1^{q-1}\}_{i=2}^s)$ .
- (b)  $F_{\mathbb{T}}(t) = (1 - t^{q-1})^{s-1}/(1 - t)^s$ .
- (c)  $\text{reg}(S/I(\mathbb{T})) = (s - 1)(q - 2)$  and  $\deg(S/I(\mathbb{T})) = (q - 1)^{s-1}$ .

When  $I(X)$  is a complete intersection, there is a general formula for the dimension of any projective Reed-Muller code arising from  $X$  [5]. For a projective torus one can easily find a formula for the dimension as shown below.

**Corollary 2.2.** [5] *If  $\mathbb{T}$  is a projective torus in  $\mathbb{P}^{s-1}$ , then the length of  $C_{\mathbb{T}}(d)$  is  $(q - 1)^{s-1}$  and its dimension is given by*

$$\dim_K C_{\mathbb{T}}(d) = \sum_{j=0}^{\lfloor \frac{d}{q-1} \rfloor} (-1)^j \binom{s-1}{j} \binom{s-1+d-j(q-1)}{s-1}.$$

*Proof.* According to Proposition 2.1, the length of  $C_{\mathbb{T}}(d)$  is  $(q - 1)^{s-1}$  and the Hilbert series of the graded algebra  $S/I(\mathbb{T})$  is given by

$$F_{\mathbb{T}}(t) = \sum_{d=0}^{\infty} H_{\mathbb{T}}(d) t^d = \frac{(1 - t^{q-1})^{s-1}}{(1 - t)^s} = \left[ \sum_{j=0}^{s-1} (-1)^j \binom{s-1}{j} t^{j(q-1)} \right] \left[ \sum_{i=0}^{\infty} \binom{s-1+i}{s-1} t^i \right].$$

Hence, comparing the coefficients of  $t^d$ , we get

$$H_{\mathbb{T}}(d) = \sum_{i+j(q-1)=d} (-1)^j \binom{s-1}{j} \binom{s-1+i}{s-1}.$$

Thus making  $i = d - j(q - 1)$  we obtain the required expression for  $\dim_K C_{\mathbb{T}}(d)$ .  $\square$

In Section 3 we compute the minimum distance of  $C_{\mathbb{T}}(d)$ , which was an important piece of information—from the viewpoint of coding theory—missing in the literature.

### 3. MINIMUM DISTANCE OF PARAMETERIZED CODES

We continue to use the notation and definitions used in the introduction. In this section we determine the minimum distance of  $C_X(d)$  when  $X$  is a projective torus in  $\mathbb{P}^{s-1}$ .

We begin with a well known and classical general upper bound.

**Lemma 3.1.** [22, Lemma 3A, p. 147] *Let  $0 \neq G = G(t_1, \dots, t_s) \in S$  be a polynomial of total degree  $d$ . Then the number  $N$  of zeros of  $G$  in  $\mathbb{F}_q^s$  satisfies*

$$N \leq dq^{s-1}.$$

*If  $G$  is homogeneous, then the number of its non-trivial zeros is at most  $d(q^{s-1} - 1)$ .*

The proof of this lemma, given in the book of W. M. Schmidt [22], can be easily adapted to obtain the following auxiliary result.

**Lemma 3.2.** *Let  $0 \neq G = G(t_1, \dots, t_s) \in S$  be a polynomial of total degree  $d$ . If*

$$Z_G := \{x \in (K^*)^s \mid G(x) = 0\},$$

*then  $|Z_G| \leq d(q-1)^{s-1}$ .*

**Lemma 3.3.** *Let  $d, d', s$  be positive integers such that  $d = k(q-2) + \ell$  and  $d' = k'(q-2) + \ell'$  for some integers  $k, k', \ell, \ell'$  satisfying that  $k, k' \geq 0$ ,  $1 \leq \ell \leq q-2$  and  $1 \leq \ell' \leq q-2$ . If  $d' \leq d$  and  $k \leq s-1$ , then  $k' \leq k$  and*

$$-(q-1)^{s-k'} + \ell'(q-1)^{s-k'-1} \leq -(q-1)^{s-k} + \ell(q-1)^{s-k-1}.$$

*Proof.* It is not hard to see that  $k' \leq k$ . It suffices to prove the equivalent inequality:

$$q-1-\ell \leq (q-1)^{k-k'}(q-1-\ell').$$

If  $k = k'$ , then  $\ell \geq \ell'$  and the inequality holds. If  $k \geq k' + 1$ , then

$$q-1-\ell \leq q-1 \leq (q-1)(q-1-\ell') \leq (q-1)^{k-k'}(q-1-\ell'),$$

as required.  $\square$

Let  $\mathbb{T}^* = (K^*)^s$  be an *affine torus*. For  $G = G(t_1, \dots, t_s) \in S$ , we denote the set of zeros of  $G$  in  $\mathbb{T}^*$  by  $Z_G$ .

**Theorem 3.4.** *Let  $G = G(t_1, \dots, t_s) \in S$  be a polynomial of total degree  $d \geq 1$  such that  $\deg_{t_i}(G) \leq q-2$  for  $i = 1, \dots, s$ . If  $d = k(q-2) + \ell$  with  $1 \leq \ell \leq q-2$  and  $0 \leq k \leq s-1$ , then*

$$|Z_G| \leq (q-1)^{s-k-1}((q-1)^{k+1} - (q-1) + \ell).$$

*Proof.* By induction on  $s$ . If  $s = 1$ , then  $k = 0$  and  $d = \ell$ . Then  $|Z_G| \leq \ell$  because a non-zero polynomial in one variable of degree  $d$  has at most  $d$  roots. Assume  $s \geq 2$ . By Lemma 3.2 we may also assume that  $k \geq 1$ . There are  $r \geq 0$  distinct elements  $\beta_1, \dots, \beta_r$  in  $K^*$  and  $G' \in S$  such that

$$G = (t_1 - \beta_1)^{a_1} \cdots (t_1 - \beta_r)^{a_r} G', \quad a_i \geq 1 \text{ for all } i,$$

and  $G'(\beta, t_2, \dots, t_s) \neq 0$  for any  $\beta \in K^*$ . Notice that  $r \leq \sum_i a_i \leq q-2$  because the degree of  $G$  in  $t_1$  is at most  $q-2$ . We can write  $K^* = \{\beta_1, \dots, \beta_{q-1}\}$ . Let  $d'_i$  be the degree of  $G'(\beta_i, t_2, \dots, t_s)$  and let  $d' = \max\{d'_i \mid r+1 \leq i \leq q-1\}$ . If  $d' = 0$ , then  $|Z_G| = r(q-1)^{s-1}$  and consequently

$$r(q-1)^{s-1} \leq (q-2)(q-1)^{s-1} \leq (q-1)^{s-k-1}((q-1)^{k+1} - (q-1) + \ell).$$

The second inequality uses that  $k \geq 1$ . Thus we may assume that  $d' > 0$  and also that  $\beta_{r+1}, \dots, \beta_m$  are the elements  $\beta_i$  of  $\{\beta_{r+1}, \dots, \beta_{q-1}\}$  such that  $G'(\beta_i, t_2, \dots, t_s)$  has positive degree. Notice that  $d = \sum_i a_i + \deg(G') \geq r + d'$ . The polynomial

$$H := (t_1 - \beta_1)^{a_1} \cdots (t_1 - \beta_r)^{a_r}$$

has exactly  $r(q-1)^{s-1}$  roots in  $(K^*)^s$ . Hence counting the roots of  $G'$  that are not in  $Z_H$  we obtain:

$$(3.1) \quad |Z_G| \leq r(q-1)^{s-1} + \sum_{i=r+1}^m |Z_{G'(\beta_i, t_2, \dots, t_s)}|.$$

For each  $r+1 \leq i \leq m$ , we can write  $d'_i = k'_i(q-2) + \ell'_i$ , with  $1 \leq \ell'_i \leq q-2$ . The proof will be divided in three cases.

Case (I): Assume  $\ell > r$  and  $k = s - 1$ . By [2, Theorem 1.2], the non-zero polynomial  $G'(\beta_i, t_2, \dots, t_s)$  cannot be the zero-function on  $(K^*)^{s-1}$  for any  $i$  because its degree in each of the variables  $t_2, \dots, t_s$  is at most  $q - 2$ . A direct argument to show that  $G'(\beta_i, t_2, \dots, t_s)$  cannot be the zero-function on  $(K^*)^{s-1}$  is to notice that if this non-homogeneous polynomial vanishes on  $(K^*)^{s-1}$ , then it must be a polynomial combination of  $t_2^{q-1} - 1, \dots, t_s^{q-1} - 1$ , a contradiction. Thus, by Eq. (3.1), we get

$$|Z_G| \leq r(q-1)^{s-1} + (q-1-r)((q-1)^{s-1} - 1) \leq (q-1)^s - (q-1) + \ell.$$

Case (II): Assume  $\ell > r$  and  $k \leq s - 2$ . Then  $d - r = k(q - 2) + (\ell - r)$  with  $1 \leq \ell - r \leq q - 2$ . Since  $d'_i \leq d - r$  for  $i = r + 1, \dots, m$ , by Lemma 3.3, we get  $k'_i \leq k$  for  $r + 1 \leq i \leq m$ . Then by induction hypothesis, using Eq. (3.1) and Lemma 3.3, we obtain:

$$\begin{aligned} |Z_G| &\leq r(q-1)^{s-1} + \sum_{i=r+1}^m |Z_{G'(\beta_i, t_2, \dots, t_s)}| \\ &\leq r(q-1)^{s-1} + \sum_{i=r+1}^m \left[ (q-1)^{(s-1)-k'_i-1} ((q-1)^{k'_i+1} - (q-1) + \ell'_i) \right] \\ &\leq r(q-1)^{s-1} + (q-1-r) \left[ (q-1)^{(s-1)-k-1} ((q-1)^{k+1} - (q-1) + (\ell-r)) \right] \\ &\leq (q-1)^{s-k-1} ((q-1)^{k+1} - (q-1) + \ell). \end{aligned}$$

Case (III): Assume  $\ell \leq r$ . Then we can write  $d - r = k_2(q - 2) + \ell_2$  with  $k_2 = k - 1$  and  $\ell_2 = q - 2 + \ell - r$ . Notice that  $0 \leq k_2 \leq s - 2$  and  $1 \leq \ell_2 \leq q - 2$  because  $k \geq 1$ ,  $r \leq q - 2$  and  $k \leq s - 1$ . Since  $d'_i \leq d - r$  for  $i > r$ , by Lemma 3.3, we get  $k'_i \leq k_2$  for  $i = r + 1, \dots, m$ . Then by induction hypothesis, using Eq. (3.1) and Lemma 3.3, we obtain:

$$\begin{aligned} |Z_G| &\leq r(q-1)^{s-1} + \sum_{i=r+1}^m |Z_{G'(\beta_i, t_2, \dots, t_s)}| \\ &\leq r(q-1)^{s-1} + \sum_{i=r+1}^m \left[ (q-1)^{(s-1)-k'_i-1} ((q-1)^{k'_i+1} - (q-1) + \ell'_i) \right] \\ &\leq r(q-1)^{s-1} + (q-1-r) \left[ (q-1)^{(s-1)-k_2-1} ((q-1)^{k_2+1} - (q-1) + \ell_2) \right] \\ &= r(q-1)^{s-1} + (q-1-r) \left[ (q-1)^{s-k-1} ((q-1)^k - (q-1) + (q-2 + \ell - r)) \right] \\ &\leq (q-1)^{s-k-1} ((q-1)^{k+1} - (q-1) + \ell). \end{aligned}$$

The last inequality uses that  $r \leq q - 2$ . This completes the proof of the result.  $\square$

We come to the main result of this section.

**Theorem 3.5.** *If  $X = \{[(x_1, \dots, x_s)] \in \mathbb{P}^{s-1} \mid x_i \in K^* \text{ for all } i\}$  is a projective torus in  $\mathbb{P}^{s-1}$  and  $d \geq 1$ , then the minimum distance of  $C_X(d)$  is given by*

$$\delta_d = \begin{cases} (q-1)^{s-(k+2)}(q-1-\ell) & \text{if } d \leq (q-2)(s-1) - 1, \\ 1 & \text{if } d \geq (q-2)(s-1), \end{cases}$$

where  $k$  and  $\ell$  are the unique integers such that  $k \geq 0$ ,  $1 \leq \ell \leq q - 2$  and  $d = k(q - 2) + \ell$ .

*Proof.* First we consider the case  $1 \leq d \leq (q - 2)(s - 1) - 1$ . Then, in this case, we have that  $k \leq s - 2$ . Let  $\prec$  be the graded reverse lexicographical order on the monomials of  $S$ . In this

order  $t_1 \succ \cdots \succ t_s$ . Let  $F$  be a homogeneous polynomial of  $S$  of degree  $d$  such that  $F$  does not vanish on all  $X$ . By the division algorithm [1, Theorem 1.5.9, p. 30], we can write

$$(3.2) \quad F = h_1(t_1^{q-1} - t_s^{q-1}) + \cdots + h_{s-1}(t_{s-1}^{q-1} - t_s^{q-1}) + F',$$

where  $F'$  is a homogeneous polynomial with  $\deg_{t_i}(F') \leq q-2$  for  $i = 1, \dots, s-1$  and  $\deg(F') = d$ . Let  $d'$  be the degree of the polynomial  $F'(t_1, \dots, t_{s-1}, 1)$ . Consider the sets:

$$\begin{aligned} Z_{F(t_1, \dots, t_{s-1}, 1)} &= \{(x_1, \dots, x_{s-1}, 1) \in (K^*)^{s-1} \times \{1\} \mid F(x_1, \dots, x_{s-1}, 1) = 0\}, \\ A_F &= \{[x] \in X \mid F(x) = 0\}. \end{aligned}$$

Notice that there is a bijection

$$Z_{F(t_1, \dots, t_{s-1}, 1)} \xrightarrow{\psi} A_F, \quad (x_1, \dots, x_{s-1}, 1) \mapsto [(x_1, \dots, x_{s-1}, 1)].$$

Indeed  $\psi$  is clearly well defined and injective. To see that  $\psi$  is onto take a point  $[x]$  in  $A_F$  with  $x = (x_1, \dots, x_s)$ . As  $F$  is homogeneous of degree  $d$ , form the equality

$$F(x_1/x_s, \dots, x_{s-1}/x_s, 1) = F(x_1, \dots, x_s)/x_s^d = 0,$$

we get that  $p = (x_1/x_s, \dots, x_{s-1}/x_s, 1)$  is a point in  $Z_{F(t_1, \dots, t_{s-1}, 1)}$  and  $\psi(p) = [x]$ . Hence  $|A_F| = |Z_{F(t_1, \dots, t_{s-1}, 1)}|$ . Using Eq. (3.2), we get  $Z_{F(t_1, \dots, t_{s-1}, 1)} = Z_{F'(t_1, \dots, t_{s-1}, 1)}$ . We set

$$H = H(t_1, \dots, t_{s-1}) = F'(t_1, \dots, t_{s-1}, 1) \text{ and } Z_H = \{x \in (K^*)^{s-1} \mid H(x) = 0\}.$$

The polynomial  $H$  does not vanish on  $(K^*)^{s-1}$ . This follows from Eq. (3.2) and using that  $F$  is homogeneous and that  $F$  does not vanish on  $X$ . We may assume that  $d' \geq 1$ , otherwise  $Z_{F'(t_1, \dots, t_{s-1}, 1)} = \emptyset$  and  $|A_F| = 0$ . Then, we can write  $d' = k'(q-2) + \ell'$  for some integers  $k' \geq 0$  and  $1 \leq \ell' \leq q-2$ . Since  $k \leq s-2$ , by Lemma 3.3, we obtain that  $k' \leq k$  and

$$(3.3) \quad -(q-1)^{s-1-k'} + \ell'(q-1)^{s-2-k'} \leq -(q-1)^{s-1-k} + \ell(q-1)^{s-2-k}.$$

Then,  $k' \leq s-2$  and  $H$  is a non-zero polynomial of degree  $d' \geq 1$  in  $s-1$  variables such that  $\deg_{t_i}(H) \leq q-2$  for  $i = 1, \dots, s-1$ . Therefore, applying Theorem 3.4 to  $H$  and then using Eq. (3.3), we derive

$$\begin{aligned} |A_F| = |Z_H| &\leq (q-1)^{s-k'-2}((q-1)^{k'+1} - (q-1) + \ell') \\ &\leq (q-1)^{s-k-2}((q-1)^{k+1} - (q-1) + \ell). \end{aligned}$$

Since  $F$  was an arbitrary homogeneous polynomial of degree  $d$  such that  $F$  does not vanish on  $X$  we obtain

$$M := \max\{|A_F| : F \in S_d; F \not\equiv 0\} \leq (q-1)^{s-k-2}((q-1)^{k+1} - (q-1) + \ell),$$

where  $F \not\equiv 0$  means that  $F$  is not the zero function on  $X$ . We claim that

$$M = (q-1)^{s-k-2}((q-1)^{k+1} - (q-1) + \ell).$$

Let  $M_1$  be the expression in the right hand side. It suffices to show that  $M$  is bounded from below by  $M_1$  or equivalently it suffices to exhibit a homogeneous polynomial  $F \not\equiv 0$  of degree  $d$  with exactly  $M_1$  roots in  $X$ . Let  $\beta$  be a generator of the cyclic group  $(K^*, \cdot)$ . Consider the

polynomial  $F = f_1 f_2 \cdots f_k g_\ell$ , where  $f_1, \dots, f_k, g_\ell$  are given by

$$\begin{aligned} f_1 &= (\beta t_1 - t_2)(\beta^2 t_1 - t_2) \cdots (\beta^{q-2} t_1 - t_2), \\ f_2 &= (\beta t_1 - t_3)(\beta^2 t_1 - t_3) \cdots (\beta^{q-2} t_1 - t_3), \\ &\vdots \\ f_k &= (\beta t_1 - t_{k+1})(\beta^2 t_1 - t_{k+1}) \cdots (\beta^{q-2} t_1 - t_{k+1}), \\ g_\ell &= (\beta t_1 - t_{k+2})(\beta^2 t_1 - t_{k+2}) \cdots (\beta^\ell t_1 - t_{k+2}). \end{aligned}$$

Now, the roots of  $F$  in  $X$  are in one to one correspondence with the union of the sets:

$$\begin{aligned} &\{1\} \times \{\beta^i\}_{i=1}^{q-2} \times (K^*)^{s-2}, \\ &\{1\} \times \{1\} \times \{\beta^i\}_{i=1}^{q-2} \times (K^*)^{s-3}, \\ &\vdots \\ &\{1\} \times \cdots \times \{1\} \times \{\beta^i\}_{i=1}^{q-2} \times (K^*)^{s-(k+1)}, \\ &\{1\} \times \cdots \times \{1\} \times \{\beta^i\}_{i=1}^\ell \times (K^*)^{s-(k+2)}. \end{aligned}$$

Therefore the number of zeros of  $F$  in  $X$  is given by

$$\begin{aligned} |A_F| &= (q-2)(q-1)^{s-2} + (q-2)(q-1)^{s-3} + \cdots + (q-2)(q-1)^{s-(k+1)} + \ell(q-1)^{s-(k+2)} \\ &= (q-1)^{s-(k+2)} \left[ (q-2)(q-1)^k + \cdots + (q-2)(q-1) + \ell \right] \\ &= (q-1)^{s-(k+2)} \left[ (q-2)(q-1)((q-1)^{k-1} + \cdots + 1) + \ell \right] \\ &= (q-1)^{s-(k+2)} \left[ (q-2)(q-1) \left( \frac{(q-1)^k - 1}{q-2} \right) + \ell \right] \\ &= (q-1)^{s-(k+2)} \left[ (q-1)^{k+1} - (q-1) + \ell \right], \end{aligned}$$

as required. Thus  $M = M_1$  and the claim is proved. Therefore

$$\begin{aligned} \delta_d &= \min\{\|\text{ev}_d(F)\| : \text{ev}_d(F) \neq 0; F \in S_d\} = |X| - \max\{|A_F| : F \in S_d; F \neq 0\} \\ &= (q-1)^{s-1} - \left( (q-1)^{s-k-2}((q-1)^{k+1} - (q-1) + \ell) \right) \\ &= (q-1)^{s-k-2}((q-1) - \ell), \end{aligned}$$

where  $\|\text{ev}_d(F)\|$  is the number of non-zero entries of  $\text{ev}_d(F)$ . This completes the proof of the case  $1 \leq d \leq (q-2)(s-1) - 1$ . Next we consider the case  $d \geq (q-2)(s-1)$ . By the Singleton bound we readily get that  $\delta_d = 1$  for  $d \geq \text{reg}(S/I(X))$ . Hence, applying Proposition 2.1, we get  $\delta_d = 1$  for  $d \geq (s-1)(q-2)$ .  $\square$

The next proposition is an immediate consequence of our result. Recall that a linear code is called *maximum distance separable* (MDS for short) if equality holds in the Singleton bound.

**Proposition 3.6.** [11, 17] *If  $X$  is a projective torus in  $\mathbb{P}^1$ , then  $C_X(d)$  is an MDS code and its minimum distance is given by*

$$\delta_d = \begin{cases} q-1-d & \text{if } 1 \leq d \leq q-3, \\ 1 & \text{if } d \geq q-2. \end{cases}$$



If  $X$  is a projective torus in  $\mathbb{P}^2$ , then the minimum distance of  $C_X(d)$  is given by

$$\delta_d = \begin{cases} (q-1)^2 - d(q-1) & \text{if } 1 \leq d \leq q-2, \\ 2q-d-3 & \text{if } q-1 \leq d \leq 2q-5, \\ 1 & \text{if } d \geq 2q-4. \end{cases}$$

Parameterized codes arising from complete bipartite graphs have been studied in [10]. In this case one can use Theorem 3.5 and the next result to compute the minimum distance.

**Theorem 3.7.** [10] *Let  $\mathcal{K}_{k,\ell}$  be a complete bipartite graph, let  $X$  be the toric set parameterized by the edges of  $\mathcal{K}_{k,\ell}$ , and let  $X_1$  and  $X_2$  be the projective torus of dimension  $\ell-1$  and  $k-1$  respectively. Then, the length, dimension and minimum distance of  $C_X(d)$  are equal to*

$$(q-1)^{k+\ell-2}, \quad H_{X_1}(d)H_{X_2}(d), \quad \text{and} \quad \delta_1\delta_2$$

respectively, where  $\delta_i$  is the minimum distance of  $C_{X_i}(d)$ .

#### 4. COMPLETE INTERSECTION IDEALS OF PARAMETERIZED SETS OF CLUTTERS

We continue to use the notation and definitions used in the introduction and in the preliminaries. In this section we characterize the ideals  $I(X)$  that are complete intersection when  $X$  arises from a clutter. Then, we show an optimal upper bound for the regularity of  $S/I(X)$ .

**Definition 4.1.** A *clutter*  $\mathcal{C}$  is a family  $E$  of subsets of a finite ground set  $Y = \{y_1, \dots, y_n\}$  such that if  $f_1, f_2 \in E$ , then  $f_1 \not\subset f_2$ . The ground set  $Y$  is called the *vertex set* of  $\mathcal{C}$  and  $E$  is called the *edge set* of  $\mathcal{C}$ , they are denoted by  $V_{\mathcal{C}}$  and  $E_{\mathcal{C}}$  respectively.

Clutters are special hypergraphs. One example of a clutter is a graph with the vertices and edges defined in the usual way for graphs.

Let  $\mathcal{C}$  be a clutter with vertex set  $V_{\mathcal{C}} = \{y_1, \dots, y_n\}$  and let  $f$  be an edge of  $\mathcal{C}$ . The *characteristic vector* of  $f$  is the vector  $v = \sum_{y_i \in f} e_i$ , where  $e_i$  is the  $i$ th unit vector in  $\mathbb{R}^n$ . Throughout this section we assume that  $v_1, \dots, v_s$  is the set of all characteristic vectors of the edges of  $\mathcal{C}$ . Recall that the algebraic toric set parameterized by  $y^{v_1}, \dots, y^{v_s}$ , denoted by  $X$ , is the set

$$X := \{[(x_1^{v_{11}} \cdots x_n^{v_{1n}}, \dots, x_1^{v_{s1}} \cdots x_n^{v_{sn}})] \in \mathbb{P}^{s-1} \mid x_i \in K^* \text{ for all } i\},$$

where  $v_i = (v_{i1}, \dots, v_{in}) \in \mathbb{N}^n$  for  $i = 1, \dots, s$ .

**Definition 4.2.** If  $a \in \mathbb{R}^s$ , its *support* is defined as  $\text{supp}(a) = \{i \mid a_i \neq 0\}$ . Note that  $a = a^+ - a^-$ , where  $a^+$  and  $a^-$  are two non-negative vectors with disjoint support called the *positive* and *negative* part of  $a$  respectively.

**Lemma 4.3.** [21, Lemma 3.4] *Let  $\mathcal{C}$  be a clutter. If  $f \neq 0$  is a homogeneous polynomial of  $I(X)$  of the form  $t_i^b - t^c$  with  $b \in \mathbb{N}$ ,  $c \in \mathbb{N}^s$  and  $i \notin \text{supp}(c)$ , then  $\deg(f) \geq q-1$ . Moreover if  $b = q-1$ , then  $f = t_i^{q-1} - t_j^{q-1}$  for some  $j \neq i$ .*

*Proof.* We may assume that  $f = t_1^b - t_2^{c_2} \cdots t_r^{c_r}$ , where  $c_j \geq 1$  for all  $j$  and  $b = c_2 + \cdots + c_r$ . Then

$$(4.1) \quad (x_1^{v_{11}} \cdots x_n^{v_{1n}})^b = (x_1^{v_{21}} \cdots x_n^{v_{2n}})^{c_2} \cdots (x_1^{v_{r1}} \cdots x_n^{v_{rn}})^{c_r} \quad \text{for all } (x_1, \dots, x_n) \in (K^*)^n.$$

We proceed by contradiction. Assume that  $b < q-1$ . We claim that if  $v_{1k} = 1$  for some  $1 \leq k \leq n$ , then  $v_{jk} = 1$  for  $j = 2, \dots, r$ , otherwise if  $v_{jk} = 0$  for some  $j \geq 2$ , then making  $x_i = 1$  for  $i \neq k$  in Eq. (4.1) we get  $(x_k^{v_{1k}})^b = x_k^b = x_k^m$ , where  $m < b$ . Then  $x_k^{b-m} = 1$  for  $x_k \in K^*$ . In particular if  $\beta$  is a generator of the cyclic group  $(K^*, \cdot)$ , then  $\beta^{b-m} = 1$ . Hence  $b-m$  is a multiple of  $q-1$  and consequently  $b \geq q-1$ , a contradiction. This completes the proof of the

claim. Therefore  $\text{supp}(v_1) \subset \text{supp}(v_j)$  for  $j = 2, \dots, r$ . Since  $\mathcal{C}$  is a clutter we get that  $v_1 = v_j$  for  $j = 2, \dots, r$ , a contradiction because  $v_1, \dots, v_r$  are distinct. Thus  $b \geq q - 1$ . The second part of the lemma follows using similar arguments (see [21]).  $\square$

A polynomial of the form  $f = t^a - t^b$ , with  $a, b \in \mathbb{N}^s$ , is called a *binomial* of  $S$ . The monomials  $t^a$  and  $t^b$  are called the *terms* of  $f$ . An ideal generated by binomials is called a *binomial ideal*.

**Theorem 4.4.** *Let  $\mathcal{C}$  be a clutter. If  $I(X)$  is a complete intersection, then*

$$I(X) = (t_1^{q-1} - t_s^{q-1}, \dots, t_{s-1}^{q-1} - t_s^{q-1}).$$

*Proof.* According to [17, Theorem 2.1] the vanishing ideal  $I(X)$  is a binomial ideal. Notice that  $I(X)$  has height  $s - 1$ . Indeed, let  $[P]$  be an arbitrary point in  $X$ , with  $P = (\alpha_1, \dots, \alpha_s)$ , and let  $I_{[P]}$  be the ideal generated by the homogeneous polynomials of  $S$  that vanish at  $[P]$ . Then

$$I_{[P]} = (\alpha_1 t_2 - \alpha_2 t_1, \alpha_1 t_3 - \alpha_3 t_1, \dots, \alpha_1 t_s - \alpha_s t_1) \quad \text{and} \quad I(X) = \bigcap_{[P] \in X} I_{[P]}$$

and the later is the primary decomposition of  $I(X)$ , because  $I_{[P]}$  is a prime ideal of  $S$  for any  $[P] \in X$ . As  $I_{[P]}$  has height  $s - 1$  for any  $[P] \in X$ , we get that the height of  $I(X)$  is  $s - 1$ . As  $I(X)$  is a complete intersection of height  $s - 1$ , there is a minimal set

$$\mathcal{B} = \{h_1, \dots, h_{s-1}\}$$

of homogeneous binomials that generate the ideal  $I(X)$ . The set  $\mathcal{B}$  is minimal in the sense that  $(\mathcal{B} \setminus \{h_i\}) \subsetneq I(X)$  for all  $i$ . We may assume that  $h_1, \dots, h_m$  are the binomials of  $\mathcal{B}$  that contain a term of the form  $t_i^{c_i}$ . By Lemma 4.3 we have that  $\deg(h_i) \geq q - 1$  for  $i = 1, \dots, m$ . Thus we may assume that  $h_1, \dots, h_k$  are the binomials of  $\mathcal{B}$  of degree  $q - 1$  that contain a term of the form  $t_i^{q-1}$  and that  $h_{k+1}, \dots, h_m$  have degree greater than  $q - 1$ . By Lemma 4.3 the binomials  $h_1, \dots, h_k$  have the form  $t_i^{q-1} - t_j^{q-1}$ . Notice that  $(I(X) : t_i) = I(X)$  for all  $i$ , this equality follows readily using that  $t_i$  does not vanish at any point of  $X$ . Hence, by the minimality of  $\mathcal{B}$ , the binomials  $h_{m+1}, \dots, h_{s-1}$  have both of their terms not in the set  $\{t_1^{a_1}, \dots, t_s^{a_s} \mid a_i \geq 1 \text{ for all } i\}$ . Since  $t_i^{q-1} - t_s^{q-1}$  is in  $I(X)$  for  $i = 1, \dots, s - 1$ , we can write

$$t_i^{q-1} - t_s^{q-1} = \sum_{\ell=1}^k \lambda_\ell h_\ell + \sum_{\ell=k+1}^m \mu_\ell h_\ell + \sum_{\ell=m+1}^{s-1} \theta_\ell h_\ell \quad (\lambda_\ell, \mu_\ell, \theta_\ell \in S).$$

As  $h_1, \dots, h_{s-1}$  are homogeneous binomials we can rewrite this equality as:

$$t_i^{q-1} - t_s^{q-1} = \sum_{\ell=1}^k \lambda'_\ell h_\ell + \sum_{\ell=m+1}^{s-1} \theta'_\ell h_\ell,$$

where  $\lambda'_\ell \in K$  for  $\ell = 1, \dots, k$  and for each  $m + 1 \leq \ell \leq s - 1$  either  $\theta'_\ell = 0$  and  $\deg(h_\ell) > q - 1$  or  $\deg(h_\ell) \leq q - 1$  and  $\deg(h_\ell) + \deg(\theta'_\ell) = q - 1$ . Then

$$t_i^{q-1} - t_s^{q-1} - \sum_{\ell=1}^k \lambda'_\ell h_\ell = \sum_{\ell=m+1}^{s-1} \theta'_\ell h_\ell.$$

The left hand side of this equality has to be zero, otherwise a non-zero monomial that occur in the left hand side will have to occur in the right hand side which is impossible because monomials occurring on the left have the form  $\lambda t_j^{q-1}$ ,  $\lambda \in K$ , and monomials occurring on the right are never of this form. Hence we get the inclusion

$$(t_1^{q-1} - t_s^{q-1}, \dots, t_{s-1}^{q-1} - t_s^{q-1}) \subset (h_1, \dots, h_k).$$

Since the height of  $(h_1, \dots, h_k)$  is at most  $k$ , we get  $s - 1 \leq k$ . Consequently  $k = s - 1$ . Thus the inclusion above is an equality as required.  $\square$

**Corollary 4.5.** *Let  $\mathcal{C}$  be a clutter with  $s$  edges and let  $\mathbb{T} = \{(x_1, \dots, x_s) \in \mathbb{P}^{s-1} \mid x_i \in K^*\}$  be a projective torus. The following are equivalent:*

- (c<sub>1</sub>)  $I(X)$  is a complete intersection.
- (c<sub>2</sub>)  $I(X) = (t_1^{q-1} - t_s^{q-1}, \dots, t_{s-1}^{q-1} - t_s^{q-1})$ .
- (c<sub>3</sub>)  $X = \mathbb{T} \subset \mathbb{P}^{s-1}$ .

*Proof.* (c<sub>1</sub>) $\Rightarrow$ (c<sub>2</sub>): It follows at once from Theorem 4.4. (c<sub>2</sub>) $\Rightarrow$ (c<sub>3</sub>): By Proposition 2.1 one has  $I(X) = I(\mathbb{T}) = (\{t_i^{q-1} - t_s^{q-1}\}_{i=1}^{s-1})$ . As  $X$  and  $\mathbb{T}$  are both projective varieties, we get that  $X = \mathbb{T}$  (see [17, Lemma 4.2] for details). (c<sub>3</sub>) $\Rightarrow$ (c<sub>1</sub>): It follows at once from Proposition 2.1.  $\square$

The next result shows that the regularity of complete intersections associated to clutters provide an optimal bound for the regularity of  $S/I(X)$ .

**Proposition 4.6.**  $\text{reg}(S/I(X)) \leq (q-2)(s-1)$ , with equality if  $I(X)$  is a complete intersection associated to a clutter with  $s$  edges.

*Proof.* For  $i \geq 0$ , we set  $h_i = \dim_K(S/(I(X), t_s))_i$ . Let  $r$  be the index of regularity of  $S/I(X)$ . Then,  $h_i > 0$  for  $i = 0, \dots, r$  and  $h_i = 0$  for  $i > r$  (see Section 2). Since  $t_s$  does not vanish at any point of  $X$ , one has  $(I(X) : t_s) = I(X)$ . Therefore, there is an exact sequence of graded  $S$ -modules

$$0 \longrightarrow (S/I(X))[-1] \xrightarrow{t_s} S/I(X) \longrightarrow S/(I(X), t_s) \longrightarrow 0,$$

where  $(S/I(X))[-1]$  is the  $S$ -module with the shifted graduation such that

$$(S/I(X))[-1]_i = (S/I(X))_{i-1}$$

for all  $i$ . Therefore from the exact sequence above we get

$$(4.2) \quad h_i = H_X(i) - H_X(i-1) \geq 0$$

for  $i \geq 1$ . On the other hand there is a surjection of graded  $S$ -modules

$$D = S/(\{t_i^{q-1} - t_s^{q-1}\}_{i=1}^{s-1} \cup \{t_s\}) = K[t_1, \dots, t_{s-1}]/(\{t_i^{q-1}\}_{i=1}^{s-1}) \longrightarrow S/(I(X), t_s) \longrightarrow 0.$$

The Hilbert series of  $D$  is equal to the polynomial  $(1+t+\dots+t^{q-2})^{s-1}$  because  $D$  is a complete intersection [29, p. 104]. Hence  $D_i = 0$  for  $i \geq (q-2)(s-1) + 1$ . From the surjection above we get that  $\dim_K D_i \geq h_i \geq 0$  for all  $i$ . If  $i \geq (q-2)(s-1) + 1$ , we obtain  $0 = \dim_K D_i \geq h_i \geq 0$ . Then, from Eq. (4.2), we conclude

$$H_X(i) = H_X(i-1) \quad \text{for } i-1 \geq (q-2)(s-1).$$

Hence  $\text{reg}(S/I(X)) \leq (q-2)(s-1)$ . To complete the proof assume that  $I(X)$  is a complete intersection, then by Corollary 4.5 the ideal  $I(X)$  is equal to  $(t_1^{q-1} - t_s^{q-1}, \dots, t_{s-1}^{q-1} - t_s^{q-1})$ . Consequently  $\text{reg}(S/I(X)) = (q-2)(s-1)$ .  $\square$

Let  $X$  be an algebraic toric set parameterized by arbitrary monomials  $y^{v_1}, \dots, y^{v_s}$ . A good parameterized code should have large  $|X|$  and with  $\dim_K C_X(d)/|X|$  and  $\delta_d/|X|$  as large as possible. The following easy result gives an indication of where to look for non-trivial parameterized codes. Only the codes  $C_X(d)$  with  $1 \leq d < \text{reg}(S/I(X))$  are interesting.

**Proposition 4.7.**  $\delta_d = 1$  for  $d \geq \text{reg}(S/I(X))$ .

*Proof.* Since  $H_X(d)$  is equal to the dimension of  $C_X(d)$  and  $H_X(d) = |X|$  for  $d \geq \text{reg}(S/I(X))$ , by a direct application of the Singleton bound we get that  $\delta_d = 1$  for  $d \geq \text{reg}(S/I(X))$ .  $\square$

A well known general fact about parameterized linear codes is that the dimension of  $C_X(d)$  is strictly increasing, as a function of  $d$ , until it reaches a constant value. This behaviour was pointed out in [5] (resp. [8]) for finite (resp. infinite) fields. The minimum distance of  $C_X(d)$  has the opposite behaviour as the following result shows.

**Proposition 4.8.** [17, 26] *If  $\delta_d > 1$  (resp.  $\delta_d = 1$ ), then  $\delta_d > \delta_{d+1}$  (resp.  $\delta_{d+1} = 1$ ).*

## ACKNOWLEDGMENTS

The authors would like to thank two anonymous referees for providing us with useful comments and suggestions, and for pointing out that Proposition 4.8 was first shown by S. Tohăneanu in [26, Proposition 2.1]. The authors would also like thank Hiram López, who provided an alternative proof of Theorem 3.5, and Carlos Rentería for many stimulating discussions.

## REFERENCES

- [1] W. W. Adams and P. Loustau, *An Introduction to Gröbner Bases*, GSM **3**, American Mathematical Society, 1994.
- [2] N. Alon, Combinatorial Nullstellensatz, Recent trends in combinatorics (Matraháza, 1995), *Combin. Probab. Comput.* **8** (1999), no. 1-2, 7–29.
- [3] E. Ballico and C. Fontanari, The Horace method for error-correcting codes, *Appl. Algebra Engrg. Comm. Comput.* **17** (2006), no. 2, 135–139.
- [4] P. Delsarte, J. M. Goethals and F. J. MacWilliams, On generalized Reed-Muller codes and their relatives, *Information and Control* **16** (1970), 403–442.
- [5] I. M. Duursma, C. Rentería and H. Tapia-Recillas, Reed-Muller codes on complete intersections, *Appl. Algebra Engrg. Comm. Comput.* **11** (2001), no. 6, 455–462.
- [6] D. Eisenbud, *The geometry of syzygies: A second course in commutative algebra and algebraic geometry*, Graduate Texts in Mathematics **229**, Springer-Verlag, New York, 2005.
- [7] D. Eisenbud and B. Sturmfels, Binomial ideals, *Duke Math. J.* **84** (1996), 1–45.
- [8] A. V. Geramita, M. Kreuzer and L. Robbiano, Cayley-Bacharach schemes and their canonical modules, *Trans. Amer. Math. Soc.* **339** (1993), no. 1, 163–189.
- [9] L. Gold, J. Little and H. Schenck, Cayley-Bacharach and evaluation codes on complete intersections, *J. Pure Appl. Algebra* **196** (2005), no. 1, 91–99.
- [10] M. González-Sarabia and C. Rentería, Evaluation codes associated to complete bipartite graphs, *Int. J. Algebra* **2** (2008), no. 1-4, 163–170.
- [11] M. González-Sarabia, C. Rentería and M. Hernández de la Torre, Minimum distance and second generalized Hamming weight of two particular linear codes, *Congr. Numer.* **161** (2003), 105–116.
- [12] M. González-Sarabia, C. Rentería and H. Tapia-Recillas, Reed-Muller-type codes over the Segre variety, *Finite Fields Appl.* **8** (2002), no. 4, 511–518.
- [13] D. Grayson and M. Stillman, *Macaulay2*, 1996. Available via anonymous ftp from [math.uiuc.edu](http://math.uiuc.edu).
- [14] J. Hansen, Linkage and codes on complete intersections, *Appl. Algebra Engrg. Comm. Comput.* **14** (2003), no. 3, 175–185.
- [15] J. Harris, *Algebraic Geometry. A first course*, Graduate Texts in Mathematics **133**, Springer-Verlag, New York, 1992.
- [16] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes*, North-Holland, 1977.
- [17] C. Rentería, A. Simis and R. H. Villarreal, Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields, *Finite Fields Appl.* **17** (2011), no. 1, 81–104.
- [18] C. Rentería and H. Tapia-Recillas, Linear codes associated to the ideal of points in  $\mathbf{P}^d$  and its canonical module, *Comm. Algebra* **24** (1996), no. 3, 1083–1090.
- [19] C. Rentería and H. Tapia-Recillas, Reed-Muller codes: an ideal theory approach, *Comm. Algebra* **25** (1997), no. 2, 401–413.

- [20] E. Reyes, R. H. Villarreal and L. Zárate, A note on affine toric varieties, *Linear Algebra Appl.* **318** (2000), 173–179.
- [21] E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, On the vanishing ideal of an algebraic toric set and its parameterized linear codes, preprint, 2010.
- [22] W. M. Schmidt, *Equations over finite fields, An elementary approach*, Lecture Notes in Mathematics **536**, Springer-Verlag, Berlin-New York, 1976.
- [23] A. Sørensen, Projective Reed-Muller codes, *IEEE Trans. Inform. Theory* **37** (1991), no. 6, 1567–1576.
- [24] R. Stanley, Hilbert functions of graded algebras, *Adv. Math.* **28** (1978), 57–83.
- [25] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.
- [26] S. Tohăneanu, Lower bounds on minimal distance of evaluation codes, *Appl. Algebra Engrg. Comm. Comput.* **20** (2009), no. 5-6, 351–360.
- [27] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic geometric codes: basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007.
- [28] A. Vardy, Algorithmic complexity in coding theory and the minimum distance problem, STOC'97 (El Paso, TX), 92109 (electronic), ACM, New York, 1999.
- [29] R. H. Villarreal, *Monomial Algebras*, Monographs and Textbooks in Pure and Applied Mathematics **238**, Marcel Dekker, New York, 2001.

DEPARTAMENTO DE MATEMÁTICAS, CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL IPN,  
APARTADO POSTAL 14–740, 07000 MEXICO CITY, D.F.

*E-mail address:* `esarmiento@math.cinvestav.mx`

DEPARTAMENTO DE MATEMÁTICA, INSTITUTO SUPERIOR TECNICO, UNIVERSIDADE TÉCNICA DE LISBOA,  
AVENIDA ROVISCO PAIS, 1, 1049-001 LISBOA, PORTUGAL

*E-mail address:* `vazpinto@math.ist.utl.pt`

DEPARTAMENTO DE MATEMÁTICAS, CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL IPN,  
APARTADO POSTAL 14–740, 07000 MEXICO CITY, D.F.

*E-mail address:* `vila@math.cinvestav.mx`